Firewall Configuration Report – task 4

Prepared by : Arti kumari

Date : 20 Nov 2025

Tool used : Ubuntu

Target System : Localhost (Windows)

1. Objective

To configure and test basic firewall rules in Windows, demonstrating how to block or allow network traffic.

2. Steps Performed

- Initial State Check: to verify the firewall's status
- Setting Default Policies and Enabling Firewall to ensure a secure posture (deny everything inbound).
- Adding Block Rule for Telnet (Port 23)
- Testing the Block Rule
- Allowing Essential Service (SSH/Port 22)
- Removing the Test Rule
- Final State Verification

3. Observations

• The custom firewall rule successfully appeared in the inbound rules list.

• Port 23 (Telnet) was blocked, ensuring that insecure Telnet connections would be denied if

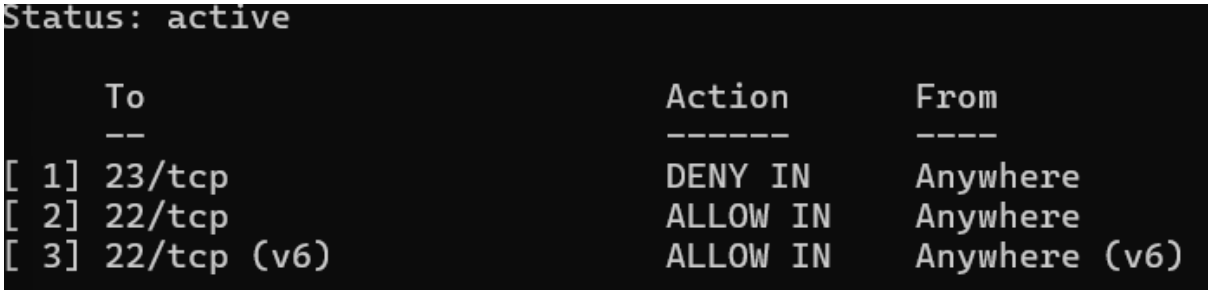
attempted.

• After deletion of the rule, the firewall returned to its default configuration

```
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     DENY IN     Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] 23/tcp (v6)                DENY IN     Anywhere (v6)
[ 4] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

After deletion



4.Conclusion

Configured and tested the **UFW firewall** on a Linux system, implementing a secure default policy (deny incoming) and demonstrating the ability to manage specific service access (blocking Telnet, allowing SSH).